Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Homomorphic Encryption and Fault Tolerant System for Personal Health Records in Cloud

Vidya .S, Sumathi .M, Ganesh .P

Assistant Professor, Department of Computer Science and Engineering,
SNS College of Technology, Coimbatore, Tamilnadu, India

Abstract— In Cloud computing the most scalable services are effortlessly utilized in an on-demand method by way of internet. Personal Health Records (PHRs) has emerged as a patient centric model of health information management and exchange. Cloud based system stores the PHRs electronically in Third Party Cloud Server. To facilitate speedy progress of cloud data storage and preserve the security assurances with outsourced PHRs, the efficient method have been planned. To promise the patients control over their own Health Records and maintain privacy, homomorphic encryption has been proposed and System trustworthiness can be enriched by the software Fault Tolerance method. The enhanced policies care about the Optimal Fault Tolerant Strategy Selection algorithm to bestow the scalable and flexible PHR Cloud applications

Keywords— Cloud Computing, PHRs, Homomorphic Encryption, Fault Tolerance.

I. INTRODUCTION

Cloud computing is a promising computing technology where applications and all the services are provided via Internet. Cloud Computing is a model for facilitating on-demand network access to collection of resources. Cloud computing paradigm offers greater elasticity and accessibility at less cost [21]. The Internet has grown into a world of its own, and its huge space now offers capabilities that could support Physicians in their duties in numerous ways. Nowadays all software functions have migrated from the local hardware to a centralized server that can be accessed from an isolated remote location. Nowadays, Cloud Computing is an emerging trend and PHR is a patient-centric model of health information exchange and management.A PHR is an electronic record of individual’s health information by which the individual controls access to the information and may have the facility to handle, follow and participate in her own health care. Generally, PHR service allows a user to build, supervise, and control her personal health data in one place through the web, which has made the storage, recovery, and distribution of the medical information more proficient. As health care professionals, physicians know that ensuring the accuracy of confidential information involves more technical approaches, to avoid the security pitfalls.

Privacy laws for the protection of patient privacy are complex and often difficult to understand in the context of an ever-growing cloud-based technology [19]. Due to the very high cost of building and maintaining precise data centres, PHR services are outsourced to or provided by third-party service providers. Example for the service providers are Microsoft Health Vault, Samedi, and Medicine Brain, etc. While it is exciting to have convenient and efficient PHR services and there are many safety and privacy risks which could impede its wide approval [20]. Outsourcing of PHR in cloud based environment relieves the burden of local data storage, retrieval and maintenance; it also eliminates their physical control of storage dependability and security. To facilitate speedy deployment of cloud data storage service and recover security assurances with outsourced data reliability, efficient methods that facilitate on-demand data correctness verification on behalf of cloud data owners have to be designed.

II. CLOUD COMPUTING IN HEALTH CARE

In general, not only the patients but doctors also could deceive by perceptions that their practices were the right ones for managing common hospitals events. In medical field cloud computing offers great prospective for speedy access to medical information. Health IT infrastructure is very complex and for this reason organization has taken additional actions to shield the organization has taken additional resources to shield the potential private data under HIPAA [3]. Maintaining secrecy and truthfulness of information stored in all forms and providing data backup, recovery and fault processes in extreme cases are extremely important. Quick access to medical history of each person at any location can speed up diagnosis and treatment quality avoiding complications increasing quality and saving life.

III. FAULT TOLERANCE STRATEGIES

The Fault Tolerant strategies have number of discrepancies based on different compositions. For every constituent in a Cloud based application, the Fault Tolerance approach discrepancies that are identified will be taken as the candidates and the optimal one needs to be identified

- Recovery Block
- N- version Programming
- Parallel

IV. Problem Statement

PHR system has multiple PHR owners and PHR users. The owners are patients who have full control over their own PHR data; they can build, control and remove the data. There is a centralized server belonging to the PHR service provider that stores all the PHR data. The users may approach from various aspects. Users may be a friend, a caregiver or a researcher. Users access the PHR documents via the server in order to read or write to someone's PHR, and a user can concurrently have access to multiple owners' data. Accuracy of the PHR in the cloud is put at threat due to the many reasons like cloud storage. Although the infrastructures under the cloud are much more dominant and trustworthy than personal computing devices, they still face a broad range of threats to data integrity [1].Outsourcing data into the cloud is economically attractive for the cost and complication of long-term large scale data storage; it does not offer any assurance on data integrity and availability. This problem, if not properly addressed, may destroy the successful deployment of the cloud architecture. To fully make sure data security and save PHR owners computation resources, propose to the framework, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed. Third party auditing provides a transparent yet cost-effective method for establishing trust between PHR owner and cloud server [2]. In fact, based on the audit result from a TPA, the released audit report would not only help PHR owners to evaluate the risk of their subscribed.

V. Proposed Architecture

The main goal of our framework is to provide secure patient-centric PHR access and efficient security and management of that data at the same time. The User data consist of users who make access based on their professional roles, such as doctors, medical officers, nurses and researchers. In practice, a user data can be mapped to an independent sector such as the health care industry, government, medical research and insurance sector.Figure 1. Proposed Architecture of PHR management it also consists of, users are personally related with a data owner and they accesses to PHRs based on access rights assigned by the owner of PHR. The architecture consists of five different entities: PHR owner, PHR user, cloud server, Third Party Auditor and Fault Tolerant Manager. PHR owner is the person whose medical information is present in that record and he has the complete rights on that data. Owner can share his information with his friends or to the doctors, nurses to get clinical suggestions.

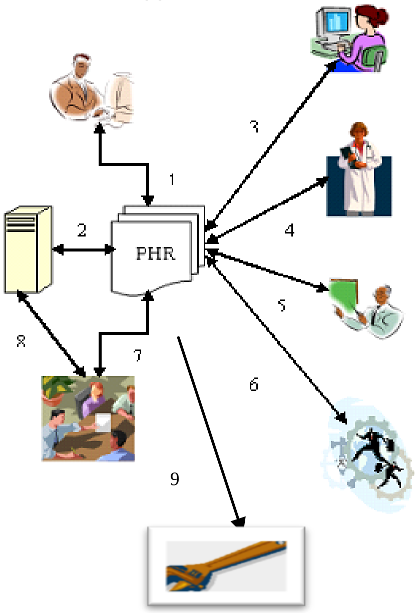

Fig 1. Proposed Architecture of PHR management

1: PHR owner access and manipulate data
2: PHR is stored in cloud server
3: Sharing with friend
4: Physician access the PHR
5: insurance company
6: emergency staff
7: third party auditing
8: cloud server
9: Fault Tolerant System

PHR user may be in personal sector or private sector [1] that has rights according to their positions with PHR owner. User can be a health care people like physicians or Friends and family members or emergency staff. Cloud server is the storage where the sensitive clinical data is stored and manipulated. It requires greater concern to maintain the data privacy and correctness. TPA is the trusted entity that has expertise and capabilities to evaluate cloud storage security and correctness on behalf of a PHR owner upon request.

The PHR owner relies on the cloud server for remote data storage and maintenance of their records, and thus is relieved of the burden of building and maintaining local storage infrastructure. In most cases cloud data storage services also provide benefits like availability, scalability, low cost and on demand sharing of data among a group of trusted users [2], such as physicians, insurance company, emergency staff, family and friends in a collaboration team or employees in the enterprise organization. As the data owner no longer possesses physical control of the data, it is of critical importance to allow the data owner to verify that his data is being correctly stored and maintained in the cloud. Assume the TPA, who is in the role of auditing, is reliable and independent, and thus has no incentive to collude with either the Cloud Servers (CS) [2] or the owners during the auditing process.

The TPA should be able to efficiently audit the cloud data storage without local copy of data and without any additional online burden for data owners. Besides, any possible leakage of an owner's outsourced PHR toward a TPA through the auditing protocol should be prohibited [2]. Both malicious outsiders and a semi-trusted CS as prospective adversaries interrupting cloud data storage services. Malicious outsiders can be economically motivated, and have the capability to attack cloud storage servers and subsequently pollute or delete owners' data while remaining undetected [12]. An encryption scheme has algorithm consists of three steps [2].

- Key Generation
- Encryption &Decryption
- Evaluation

Utilizing Homomorphic Authenticators [12]to significantly reduce the arbitrarily large communication Overhead for public auditability without introducing any online burden on the data owner, resort to the homomorphic authenticator technique Homomorphic authenticators are unforgeable metadata generated from individual data blocks, which can be securely aggregated in such a way to assure a verifier that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator[2].

FTM is built to work on top of the hyper visor, spanning all the nodes and navigating the generalization layers of the Cloud to translucently tolerate failures among the progressing nodes [6]. Fig.2 depicts the architecture of FTM which can primarily be viewed as a collection of several web service constituents, each with a specific functionality. A concise explanation of the functionality of all the constituents along with the underlying principle behind their enclosure in the framework is provided further in this section.

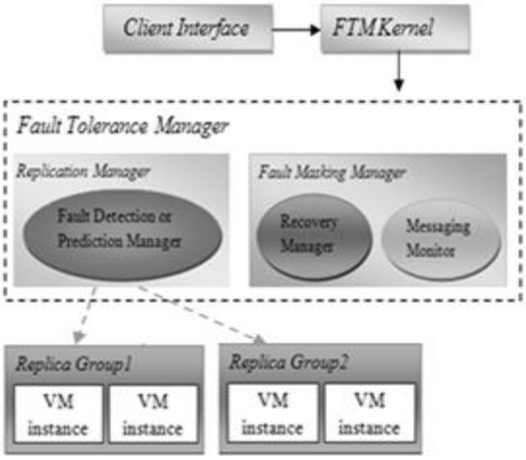

Fig 2 Fault tolerant System

The main mission of the messaging monitor is that it broadens through all the major constituents of our proposed framework and offers the mere communication level infrastructure in two different formats: message level type exchange within each replica group and inter constituent level type communication form within the framework. FTM Kernel selects an appropriate messaging strategy while making a Fault Tolerance type algorithm such that an autonomous service of messaging facility is available for each instance.

VI. CONCLUSIONS

This paper discusses about the Development in patient centric model and cloud computing in PHR management. This requires the trustworthy service in cloud to protect the precious patient data.PHR is used by multiple users so it requires the more security and privacy to reduce the complexity and reliability. Proposed system uses the TPA auditing to verify the cloud server which used to store and process the PHR and homomorphic encryption with data auditing is used to verify the trustworthiness of TPA. Cloud computing security is very challenging and very essential one because it attracts numerous applications. This approach also incorporates Fault Tolerance mechanisms as self regulating modules, validating Fault Tolerance possessions of each mechanism, and complementing customer's necessities with available Fault Tolerance modules to obtain a far-reaching solution with desired possessions. After finding out the momentous constituents Optimal Fault Tolerance Strategy Selection algorithm to provide optimal Fault Tolerance mechanisms to the momentous constituents automatically, based on the user constrictions. The future work can be extended to include more users and to develop the approaches to security handle contemporary threats in cloud based system.

REFERENCES

[1] Ravi Jhawar, Vincenzo Piuri, and Marco Santambrogio, “Fault Tolerance Management in Cloud Computing: A System- Level Perspective”, IEEE systems journal, vol. 7, no. 2, June 2013.

[2] Wenbing Zhao, IEEE, Melliar-Smith P. M. and Moser L. E., IEEE, “Fault Tolerance Middleware for Cloud Computing”, 2010 IEEE 3rd International Conference on Cloud Computing.

[3] Prasenjit Kumar Patra, Harshpreet Singh, Gurpreet Singh, “Fault Tolerance Techniques and Comparative Implementation in Cloud Computing”, IJCA, February 2013.

[4] Anjali D.Meshram, A.S. Sambare, S.D.Sade, “Fault Tolerance Model for Reliable Cloud Computing”, IJRITCC July 2013.

[5] Sheheryar Malik, IEEE, Fabrice Huet, IEEE, “Adaptive Fault Tolerance in Real Time Cloud Computing”, 2011 IEEE World Congress on Services.

[6] Ravi Jhawar, Vincenzo Piuri, and Marco Santambrogio, “A Comprehensive Conceptual System- Level Approach to Fault Tolerance in CloudComputing”, 2012 IEEE International Systems Conference.

[7] Amazon elastic compute Cloud.

[8] Alain Tchana, Laurent Broto, Daniel Hagimont “Approaches to Cloud Computing Fault Tolerance”, IEEE 2012 International Conference.

[9] Zibin Zheng and Michael R. Lyu, “Optimal Fault Tolerance Strategy Selection for Web Services”, IJWSR 2010.

[10] Zibin Zheng and Michael R. Lyu, “A QoS Aware Fault Tolerant Middleware for Dependable Service Composition”
IEEE International Conference 2009.

[11] N-Version Programming www.hillside.net/plop/2009/Process/N-Version Programming.pdf.

[12] Vidya, S., K. Vani, and D. Kavinpriya. "Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing." International Journal of Engineering 1.10 (2012)

[13] A. Vetro, H. Sun, P. DaGraca, and T. Poon, “Minimum drift architectures for three-layer scalable DTV decoding,” IEEE Trans. Consumer Electron., vol. 44, no. 3, pp. 527-536, Aug. 1998.

[14] Ming Li, Shucheng Yu, Yao Zheng, , Kui Ren, Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption” IEEE Transactions on Parallel and Distributed Systems,2012.

[15] Carolina A. Klein, MD, “Cloudy Confidentiality: Clinical and Legal Implications of Cloud Computing in Health Care” The Journal of the American Academy of Psychiatry and the Law, pp.571-578, 2011.

[16] Zhiguo Wan, Jun’e Liu, and Robert H. Deng, “HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing”, IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, Pp. 743-754, April 2012

[17] Cong Wang and Kui Ren, Jin Li, “Toward Publicly Auditable Secure Cloud Data Storage Services”, IEEE Network, pp. 19-24,July/August 2010.

[18] Carlos Oberdan Rolim, Fernando Luiz Koch, Carlos Becker Westphall, Jorge Werner, Armando Fracalossi, Giovanni Schmitt Salvador, “A Cloud Computing Solution for Patient’s Data Collection in Health Care Institutions”, Journal of Emerging Trends in Computing and Information Sciences”

[19] Aderemi A. Atayero*, Oluwaseyi Feyisetan, “Security Issues in Cloud Computing: The Potentials of Homomorphic
Encryption”, Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, pp. 546-552, October 2011

[20] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in SecureComm’10, Sept. 2010, pp. 89–106.

[21] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the ehealth cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI ’10, 2010, pp. 220–229.

[22] M.Li, S.Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in ICDCS ’11, Jun. 2011.

[23] C.Wang et al.,”Ensuring Data Storage Security in Cloud Computing,” Proc. IWQoS ‘09, July 2009, pp. 1–9. [13] Q.Wang et al., “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. ESORICS ‘09, Sept. 2009, pp. 355–70.

[24] C. Erway et al., “Dynamic Provable Data Possession,” Proc. ACM CCS ‘09, Nov. 2009, pp. 213–22.

[25] C.Wang et al., “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ‘10, Mar.2010.

[26] R.C.Merkle, “Protocols for Public Key Cryptosystems,” Proc.IEEE Symp. Security Privacy, 1980